

---

## **Sicherheitsgefahren durch unzureichenden Schutz mit nur einer Anti-Viren-Engine**

---

Warum sich nach Virenausbrüchen Wartezeiten bei Signatur-Updates nur mit mehreren Engines sicher überbrücken lassen

Eine einzelne Anti-Viren-Engine, die Viren, Trojaner und andere Bedrohungen stets am schnellsten und effektivsten erkennt, ist noch nicht erhältlich. Dieses White Paper erläutert, warum daher nur durch den gleichzeitigen Einsatz mehrerer Viren-Scanner auf E-Mail-Server-Ebene sich die Gefahr des Eindringens von Viren bedeutend mindern lässt.

## Einführung

Viren, Trojaner, Würmer, Spam-Nachrichten und andere Arten von Malware stellen eine große Bedrohung für Unternehmen und Organisationen aller Art dar, da sie die Sicherheit und Integrität vertraulicher und unternehmenskritischer Daten gefährden und zudem die Produktivität einschränken. Der Schutz der E-Mail-Kommunikation sollte für Firmen weiterhin oberste Priorität haben: Laut der FBI-Studie „2006 CSI/FBI Crime and Security Survey“ setzten 97 % der befragten Unternehmen Anti-Viren-Software ein – dennoch hatten 65 % im untersuchten Zeitraum von zwölf Monaten mindestens ein Mal mit Schädlingen zu kämpfen gehabt. Laut von Network World zitierten Studien beliefen sich die Kosten zur Abwehr von per E-Mail verbreiteten Schädlingen wie Blaster, SoBig.F und Sober allein für US-Unternehmen auf US-\$ 3,5 Mrd. Eine von der britischen Regierung im Jahr 2006 in Auftrag gegebene Studie ergab, dass 43 % der Unternehmen in Großbritannien im Vorjahr einen Virenbefall ihrer Systeme zu verzeichnen hatten.

Verantwortungsbewusste Organisationen wissen, dass sich ihr Netzwerk nur durch die Verwendung einer E-Mail-Sicherheitslösung sinnvoll vor böswilligen Virenangriffen schützen lässt. Diese Lösung muss dazu in der Lage sein, den immer raffinierteren Schadcode zu erkennen, der von Virenschreibern kontinuierlich weiterentwickelt wird, um Viren-Scanner und Firewalls zu überwinden. Viren sind vor allem so erfolgreich, weil Abwehrmaßnahmen nicht durchdacht genug sind und grundlegende Schwächen aufweisen, vor allem, wenn nur eine einzige Scan-Engine zur Kontrolle eingehender Nachrichten eingesetzt wird.

Dieses White Paper erläutert, warum sich interne Netzwerke allein durch den Einsatz einer einzelnen Anti-Viren-Engine nicht hinreichend vor Mass-Mailing-Viren, Würmern und anderen per E-Mail verbreiteten Gefahren absichern lassen. Zudem erfahren Sie, warum nach einem Virenausbruch die durchschnittliche Wartezeit für aktualisierte Virensignaturen nur mit mehreren Anti-Viren-Engines minimiert werden kann – und somit die Infektionsgefahr sinkt. Des Weiteren wird darauf eingegangen, warum der Einsatz mehrerer Anti-Viren-Engines Administratoren eine größere Unabhängigkeit beim Viren-Scanning bietet und es ermöglicht, Scan-Engines zu verwenden, die sich als am leistungsfähigsten erwiesen haben.

Einführung .....	2
Warum schnelle Reaktionszeiten so wichtig sind .....	3
Fallstudie: Reaktionszeiten bei Varianten des Sober-Wurms .....	3
Kombinieren von Abwehrtechnologien .....	5
Argumente für den Einsatz mehrerer Anti-Viren-Engines .....	5
Neue Sicherheitsstrategie .....	7
Über GFI MailSecurity for Exchange/SMTP .....	7
Über GFI .....	8

---

## Warum schnelle Reaktionszeiten so wichtig sind

Ob ein Netzwerk erfolgreich vor Viren geschützt werden kann, hängt maßgeblich davon ab, wie schnell die Virensignaturen eines Scanners nach einem neuen Virenausbruch aktualisiert und vom Anbieter der Abwehr-Engine bereitgestellt werden. Die weltweite Verbreitung von Schädlingen per E-Mail erfolgt innerhalb weniger Stunden, und ein einziger über die elektronische Post eingeschleppter Schädling reicht bereits aus, um ein ganzes Netzwerk zu infizieren. Daher ist es umso wichtiger, dass aktualisierte Signaturdateien so schnell wie möglich verfügbar gemacht werden. Kommt ein neuer Virus in Umlauf, sind Systeme so lange ungeschützt, bis der Anti-Viren-Hersteller neue Signaturen übermittelt. Je schneller die Aktualisierung erfolgt, desto geringer das Risiko, dass der neue Schädling in das Unternehmensnetzwerk eindringt. Eine von der britischen Regierung im Jahr 2006 in Auftrag gegebene Studie ergab, dass alle größeren Unternehmen in Großbritannien zwar Anti-Viren-Produkte einsetzen, 43 % von ihnen aber dennoch im Jahr 2005 von Viren infiziert wurden – vorrangig, weil die Bereitstellung von Signatur-Updates nicht schnell genug erfolgt war.

Jeder Anti-Viren-Hersteller behauptet, am schnellsten auf neue Viren reagieren und Updates noch vor allen anderen Wettbewerbern zur Verfügung stellen zu können. In der Praxis ergibt sich jedoch ein anderes Bild. Anti-Viren-Hersteller stellen aktualisierte Signaturdateien nach neuen Viren- oder Wurmausbrüchen in nur sehr unregelmäßigen Zeitabständen bereit. Es kann beispielsweise vorkommen, dass ein- und derselbe Hersteller bereits innerhalb von sechs Stunden nach Bekanntwerden eines neuen Schädlings die neuesten Updates liefert – in einem anderen Fall können wiederum achtzehn Stunden vergehen, bis dieser Hersteller reagiert. Es gibt zwar einige Hersteller, die im Allgemeinen schneller auf Virenausbrüche reagieren als ihre Mitbewerber, aber keinen, der stets als Erster seine Updates zur Verfügung stellt. Kaspersky, McAfee, BitDefender, Norman und andere Anti-Viren-Hersteller stehen daher mit ihren Response-Zeiten abwechselnd an der Spitze.

Eine Verzögerung bei der Veröffentlichung aktualisierter Signaturdateien ist zudem nicht auf Qualität und Kompetenz von Anti-Viren-Herstellern zurückzuführen, sondern auf den Standort ihrer Forschungslabore in unterschiedlichen Zeitzonen.

---

## Fallstudie: Reaktionszeiten bei Varianten des Sober-Wurms

Die folgenden Tabellen informieren, nach wie vielen Stunden die einzelnen Anti-Viren-Hersteller mit ihren Updates auf zwei neue Versionen des Sober-Wurms reagiert haben.

**Tabelle 1 – Reaktionszeiten v. Anti-Viren-Herstellern auf den Ausbruch von w32.Sober.C**

Hersteller	Reaktionszeit in Stunden
BitDefender	10,5
Kaspersky	12,0
F-Prot (Frisk)	12,5
F-Secure	13,0
Norman	15,5
eSafe (Alladin)	15,5
TrendMicro	17,0
AVG (Grisoft)	17,5
AntiVir (H+BEDV)	19,5
Symantec	25,0
Avast! (Alwil)	31,0
Sophos	35,5
Panda AV	38,0
McAfee/NAI	49,0
Ikarus	56,5

Reaktionszeit: 10,5 Stunden - 56,5 Stunden. Median: 17,5 Stunden. Durchschnitt: 24,53 Stunden. Quelle: VirusBTN, Ausgabe Februar 2004

**Tabelle 2 – Reaktionszeiten v. Anti-Viren-Herstellern auf den Ausbruch von w32.Sober.Y**

Hersteller	Reaktionszeit in Stunden
AntiVir	11,5
McAfee/NAI	40,5
Kaspersky	43,0
Norman	60,0
BitDefender	114,5
Symantec	116,0
ClamAV	164,5
TrendMicro	168,0
Panda	168,0
Sophos	170,0

Reaktionszeit: 11,5 Stunden - 170,0 Stunden. Median: 115,75 Stunden. Durchschnitt: 105,6. Quelle: av-Test.de, November 2005

Wie deutlich zu sehen ist, reicht die Reaktionszeit von ein paar Stunden bis zu mehreren Tagen – es bleibt daher ein großes Risiko, dass das Netzwerk in der Zwischenzeit infiziert wird.

---

## Kombinieren von Abwehrtechnologien

Die verschiedenen Anti-Viren-Hersteller und Scan-Engines unterscheiden sich in mehreren Aspekten. Jeder Viren-Scanner hat seine Stärken und Schwächen, es gibt keine Lösung die stets den besten Schutz bietet. Um Schädlinge erkennen und abwehren zu können, kommen bei vielen Produkten mehrere Schutztechnologien gleichzeitig zum Einsatz.

Zu den drei am häufigsten verwendeten Abwehrmaßnahmen zählen:

- **Signaturdateien**, die von Anti-Viren-Herstellern regelmäßig erstellt und veröffentlicht werden und bei der Identifizierung von Viren helfen. Die Aktualisierung von Anti-Viren-Engines erfolgt üblicherweise über diese Art von Dateien.
- **Heuristiken** kommen zum Einsatz, um Viren und andere Bedrohungen zu erkennen, für die noch keine aktualisierten Signaturdateien verfügbar sind. Bei dieser Technologie werden verschiedene Charakteristika einer Datei untersucht. Solche, die auf einen Schadteil schließen lassen, werden als gefährlich klassifiziert. Zudem lassen sich mit dieser Methode Metamorphose-Viren, die mutieren und dabei ihre äußere Form ändern können, identifizieren und abfangen. Diese Art von Schädlingen lässt sich mit Hilfe normaler Signaturdateien so gut wie nicht erkennen.
- **Sandbox-Technologie**, die verdächtigen Code isoliert und über einen virtuellen Rechner, der von der übrigen IT-Infrastruktur getrennt ist, ausführt um festzustellen, ob er böswillig ist.

Diese einzelnen Technologien können sehr effektiv sein, jedoch bietet keine von ihnen 100-prozentigen Schutz. Bei einigen Anti-Viren-Lösungen werden diese Technologien miteinander kombiniert, jedoch gibt es auch hier kein einzelnes Produkt, das sich von allen anderen absetzt. Abwehr und Sicherheit mit bestmöglichem Schutz werden nur durch mehrere Ebenen der Verteidigung erzielt – durch den Einsatz mehrerer Anti-Viren-Engines.

---

## Argumente für den Einsatz mehrerer Anti-Viren-Engines

PC SecurityShield schätzt, dass tagtäglich mehr als 40 neue Viren entdeckt werden. Im Juni 2006, so Microsoft, war ein Rechner pro 300 PCs mit Malware infiziert. Malware wird fortlaufend von einer Unzahl an Virenschreibern weiterentwickelt, von denen jeder seine eigenen Angriffsmethoden und unterschiedliche Ziele verfolgt – entsprechend groß ist die Herausforderung, eine geeignete Abwehrstrategie zu finden.

Für den Einsatz gleich mehrerer Anti-Viren-Engines spricht das oben bereits angeführte Argument, dass es keine einzelne Engine gibt, mit der alle Gefahren abgewehrt werden können,

denn ein Virenblocker, der stets am schnellsten, effektivsten und „besten“ ist, steht nicht zur Verfügung. Bei einer Engine, die mit den kürzesten durchschnittlichen Reaktionszeiten aufwartet, ist noch längst nicht garantiert, dass diese auch beim nächsten Virenausbruch den schnellsten Schutz bietet. Ebenso ist es wenig aussagekräftig, wenn diese Engine bei einem bestimmten Virus einmal nicht schnell genug aktualisiert werden konnte oder nicht die richtige Auswahl an Technologien oder Heuristiken besaß. Es zählt allein, dass das einmalige Versagen der Engine ausreicht, um ein Netzwerk zu infizieren und großen Schaden anzurichten. Die Konsequenzen einer Infizierung und möglicher Systemabstürze sind verheerend: Produktivitätsverlust, Umsatzeinbußen, Nichterreichbarkeit für Kunden, hohe Kosten für die Schadensbehebung u. v. m.

Es kann auch vorkommen, dass Aktualisierungen der Anti-Viren-Engine fehlerhaft sind, da Hersteller Updates immer unter Zeitdruck entwickeln und verbreiten. Werden mehrere Engines gleichzeitig verwendet, können Fehlfunktionen einer der Engines leichter kompensiert werden, und es besteht weiterhin ein wirksamer Schutz.

### **Hinweis zur Benutzung mehrerer Anti-Viren-Engines**

Obwohl die gleichzeitige Verwendung mehrerer Anti-Viren-Lösungen hervorragende Abwehrmöglichkeiten bietet, ist jedoch ein Aspekt zu beachten: Es darf nicht irrtümlich angenommen werden, dass bei fünf Viren-Scannern auch ein fünffacher Schutz zu erwarten ist. Es stehen fünf Möglichkeiten für eine korrekte Antwort auf Bedrohungen bereit, und jede einzelne Möglichkeit ist statistisch gesehen als unabhängiges Ereignis zu werten. Diese Struktur kann mit fünf aufeinander folgenden Flughafen-Sicherheitskontrollen verglichen werden, bei denen jede mehr oder weniger gleich ist, sich aber dennoch in ihrer Ausführung geringfügig von den anderen unterscheidet – und somit die Chance erhöht, eine Gefahr aufzuspüren und diese rechtzeitig abzuwehren.

### **Versagen von Verteidigungsmaßnahmen bei Dauerangriffen**

Die anfangs erwähnte CSI/FBI-Studie, bei der 65 % der Teilnehmer angaben, in den zwölf Monaten vor der Befragung mindestens ein Mal von Computer-Viren betroffen gewesen zu sein, kam zu dem Ergebnis, dass US-Unternehmen hierdurch Schäden in Höhe von insgesamt fast sechzehn Millionen US-Dollar entstanden sind – obwohl fast alle Befragten branchenweit anerkannte Anti-Viren-Lösungen in ihren Unternehmen eingesetzt hatten. Dies lässt den beinahe eindeutigen Schluss zu, dass die Infizierung der Systeme auf den Einsatz von nur einer Anti-Viren-Engine zurückzuführen ist, deren Dienste im entscheidenden Moment versagt haben.

## **Vielschichtiger Schutz in allen Bereichen der Sicherheit**

Unternehmen vertrauen beim Schutz von Firmengebäuden üblicherweise immer auf mehrere Sicherheitsmaßnahmen wie umfangreiches Sicherheitspersonal oder redundante Alarmsysteme, um auf Gefahren wie Diebstahl, Vandalismus, Feuer oder Ähnliches vorbereitet zu sein. Eine umfassende Absicherung sollte in gleichem Maße auch für Unternehmensdaten gelten, deren Wert ungleich höher ist – diesen Schutz können jedoch nur mehrere Anti-Viren-Engines bieten, die gleichzeitig ihren Dienst versehen. Sein Vertrauen auf andere Methoden zu setzen, wäre höchst fahrlässig.

---

## **Neue Sicherheitsstrategie**

Dieses White Paper verdeutlicht, dass eine einzige Anti-Viren-Engine nicht ausreicht, um ein Netzwerk vor Schädlingen zu schützen. Unternehmen müssen eine vielschichtige Scan-Lösung einsetzen, die gleich mehrere Anti-Viren-Engines bietet und hierdurch Wartezeiten bei Signatur-Updates möglichst gering hält. Nur so lassen sich die Chancen steigern, dass mindestens eine von ihnen schnell genug aktualisiert wird, bevor ein Virus zuschlagen kann. Ebenso ist mit mehreren Scannern die Wahrscheinlichkeit größer, die richtige Kombination aus Abwehrtechnologien zu besitzen, die einen größtmöglichen Schutz vor Gefahren bietet.

Durch Verwendung einer Lösung wie GFI MailSecurity for Exchange/SMTP, die den gleichzeitigen Einsatz von bis zu fünf Anti-Viren-Engines unterstützt, bestehen weitaus umfangreichere Möglichkeiten eines effektiven und vor allem rechtzeitigen Netzwerkschutzes – auch, weil Unternehmen sich nicht länger auf einen einzigen Hersteller verlassen und darauf hoffen müssen, dass dieser am schnellsten und wirkungsvollsten reagiert.

---

## **Über GFI MailSecurity for Exchange/SMTP**

GFI MailSecurity for Exchange/SMTP ist eine umfassende E-Mail-Sicherheitslösung und bietet Exploit-Erkennung, Gefahrenanalyse und Anti-Viren-Schutz für elektronische Post. Sämtliche schädlichen Elemente, die sich per E-Mail übertragen lassen, werden beseitigt, bevor sie Anwender erreichen. Zum Scannen von E-Mails setzt GFI MailSecurity mehrere Anti-Viren-Engines ein, darunter Kaspersky, McAfee, BitDefender, Norman und GRISOFT AVG Anti-Virus. Zu den weiteren wichtigen Leistungsmerkmalen zählen Module zur Inhalts- und Anhangskontrolle von E-Mails, um gefährliche Inhalte und Anhänge unter Quarantäne zu stellen, die Email Exploit Engine zur Abwehr von aktuellen und zukünftigen auf Exploits basierenden Viren (z. B. Nimda, Bugbear), den HTML Sanitizer zum Bereinigen von HTML-Skripten sowie der Trojan & Executable Scanner zum Aufspüren potenziell gefährlicher exe-Dateien. Weitere Informationen und eine kostenfreie Test-Version von GFI MailSecurity finden Sie unter [www.gfisoftware.de/de/mailsecurity](http://www.gfisoftware.de/de/mailsecurity).

---

## Über GFI

GFI Software bietet als führender Software-Hersteller eine umfassende Auswahl an Netzwerksicherheits-, Inhaltssicherheits- und Kommunikationslösungen aus einer Hand, um Administratoren einen reibungslosen Netzwerkbetrieb zu ermöglichen. Mit seiner mehrfach ausgezeichneten Technologie, einer konsequenten Preisstrategie und der Ausrichtung an den Anforderungen kleiner und mittlerer Unternehmen erfüllt GFI höchste Ansprüche an Effizienz und Produktivität. Das Unternehmen wurde 1992 gegründet und ist mit Niederlassungen auf Malta, in London, Raleigh, Hongkong, Adelaide sowie auf Hamburg vertreten und betreut über 200.000 Installationen weltweit. GFI bietet seine Lösungen über ein weltweites Netz von mehr als 10.000 Channel-Partnern an und ist Microsoft Gold Certified Partner. Weitere Informationen stehen zum Abruf bereit unter <http://www.gfisoftware.de>.

© 2007. GFI Software. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI Software zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema dieses White Papers wieder. Modifizierungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI Software dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Die Angaben in diesem White Paper dienen nur der allgemeinen Information. GFI Software übernimmt keine ausdrückliche oder stillschweigende Haftung für die in diesem Dokument präsentierten Informationen. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor und die zugehörigen Produktlogos sind eingetragene Marken oder Marken von GFI Software in den Vereinigten Staaten und/oder anderen Ländern. Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.